UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

GOMIAN KONNEH, on behalf of herself and all others similarly situated, Plaintiff, v. URBAN ONE, INC., Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Gomian Konneh ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Urban One, Inc., ("Urban One" or "Defendant"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

INTRODUCTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. US-based media conflomerate Urban One lost control over its computer network and cybercriminals accessed highly sensitive personal information including at least full names, Social Security numbers, home addresses, direct deposit information, and W-2 information ("PII").

3. On information and belief, Defendant's computer systems were accessed by the notorious cybercriminal group Cactus ***for over a month***, starting around February 13, 2025 ("the Data Breach"). Exhibit 1.

4. During this cyberattack Cactus stole at least 2.5 TB of data containing sensitive information belonging to Urban One's current and former employees, and posted a sample of documents—including a passport, contracts, and income statements—on its leak site to back its

claims. Cactus alleges the 2.5 TB of data includes much more than Urban One disclosed, such as personal identifiable information, database backups, corporate internal documents, contracts, agreements, financial data/payroll, legal documents, employees and executives' personal data, corporate confidential and personal correspondence, etc.

5. The Data Breach impacted an unknown number of individuals all over the United States. Notifications have already been to sent to residents in Massachusetts, Texas, Maryland, and Pennsylvania, and additional disclosures are expected as investigations continue.

6. Upon information and belief, Cactus was able to breach Urban One's systems because Urban One failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering it an easy target for cybercriminals.

7. The fact it took Urban One over a month to discover cybercriminals were stealing sensitive information from its computer systems underscores its complete and utter failure to maintain reasonable security safeguards to protect PII.

8. Urban One's failure to maintain reasonable security safeguards is all the more egregious considering it previously informed California regulators of a data breach in 2019 that involved the theft of more than 1,000 Social Security numbers, when it promised "it is taking steps, including strengthening its network security posture, to prevent a similar event from occurring in the future."[1]

[1] *Submitted Breach Notification Sample,* ROB BONTA ATTORNEY GENERAL https://oag.ca.gov/ecrime/databreach/reports/sb24-146060 (last visited May 5, 2025)

9. Urban One obfuscates the nature of the Data Breach and the threat it posed, publicly claiming that no financial account information was compromised, although Plaintiff's breach notice indicates her direct deposit information and W-2 was compromised. Moreover, Urban One's decision to involve federal law enforcement and cybersecurity firm Mandiant indicates the seriousness of the attack. Moreover, Urban One

10. In failing to adequately protect its former and current employees' information, adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its current and former employees.

11. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust when Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff Gomian Konneh is a victim of the Data Breach. On information and belief, her at least her full name, Social Security number, home address, direct deposit information, and W-2 information were exposed in the Data Breach.

13. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

14. Plaintiff seeks, on behalf of herself and the Class, monetary damages and injunctive relief including lifetime credit monitoring and ID theft monitoring.

PARTIES

15. Plaintiff Gomian Konneh is a natural person and citizen of Philadelphia, Pennsylvania, where she intends to remain.

16. Defendant Urban One, Inc. is a business corporation incorporated in Maryland, with its principal place of business at 1010 Wayne Avenue, 14th Floor, Silver Springs, Maryland 20910.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; and Plaintiff and Defendant are citizens of different states.

18. This Court has personal jurisdiction over Defendants because Defendants maintain their principal place of business in this District and do substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

20. Urban One is a multi-media production and distribution company based in Maryland. For over 40 years, Urban One's mission is to be a trusted source in the African-American community that informs, entertains and inspires its audience by providing culturally relevant integrated content through radio, television, and digital platforms.[2] Today, Urban One's brands include TV One, CLEO TV, Radio One, Reach Media, iOne Digital, One Solution, and R1 Digital.[3]Headquartered in Silver Spring, Maryland, Urban One employs over 1000 individuals.[4]

[2] *We are Urban One,* URBAN ONE., https://urban1.com/company/ (last visited May 5, 2025).
[3] *Urban One,* URBAN ONE., https://urban1.com/ (last visited May 5, 2025).
[4] *Urban One, Inc.,* LINKEDIN, https://www.linkedin.com/company/urban-one-inc/about/ (last visited May 5, 2025).

21. On information and belief, Urban One accumulates highly private PII of its employees. Urban One has accrued nearly 40 years of data and contracts.

22. In collecting and maintaining its employees' PII, Urban One agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

23. Urban One understood the need to protect its current and former employees' PII and prioritize its data security.

24. Urban One emphasizes the importance of data security in its privacy policy, stating "Urban One, Inc. and its family of affiliate and subsidiary entities…respect your privacy" and "We maintain procedural, technical, and physical safeguards to help protect against loss, misuse, or unauthorized access, disclosure, alteration, or destruction of the Personal Information you provide via the Urban One Services."[5]

25. Despite recognizing its duty to do so, and despite being no stranger to data breaches, on information and belief, Urban One has not implemented reasonable cybersecurity safeguards or policies to protect the PII of its current and former employees, or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Urban One leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

Defendant Failed to Safeguard the PII of Plaintiff and the Class

26. Plaintiff is a former employee of Defendant.

27. Plaintiff received Defendant's Notice on or around April 18, 2025, informing her that her PII was compromised.

[5] *Privacy Policy,* URBAN ONE PRIVACY POLICY, https://urban1.com/privacy/ (last visited May 5, 2025).

28. Plaintiff was surprised to have received this notice because she reasonably believed that her data would have been destroyed or deleted once her employment with Urban One ended.

29. As a condition of receiving employment from Defendant, Plaintiff provided Defendant with her PII.

30. On information and belief, Defendant collects and maintains its current and former employees' unencrypted PII in its computer systems.

31. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law.

32. Starting February 13, 2025, and continuing for an unknown length of time, cybercriminals hacked Defendant's network and accessed extremely sensitive information, including full names, Social Security numbers, home addresses, direct deposit information, and W-2 information. Exhibit 1.

33. While Defendant claims to have discovered the Data Breach on March 15, 2025, Defendant has not publicly disclosed when it was able to stop the Data Breach. *Id.*

34. Defendant obfuscates the nature of the Data Breach, publicly claiming that financial account information was not impacted,[6] although the breach notice indicates her direct deposit information and W-2 were impacted. *Id.*

35. Defendant has not publicly disclosed the severity of the Data Breach, although Urban One's decision to involve federal law enforcement and cybersecurity firm Mandiant indicates the seriousness of the attack.[7]

---

[6] *Urban One Hit by Ransomware: Employee Data Leaked,* NATIONAL CYBER SECURITY, https://nationalcybersecurity.com/urban-one-hit-by-ransomware-employee-data-leaked-ransomware-cybercrime/?utm_source=rss&utm_medium=rss&utm_campaign=urban-one-hit-by-ransomware-employee-data-leaked-ransomware-cybercrime (last visited May 5, 2025).

[7] *Id.*

36. Defendant has not publicly disclosed whether it paid the ransom for its employees data, and Cactus' post on its leak site suggests it has not.

37. Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to peruse and obtain files ***for over a month*** containing a treasure trove of thousands of its employees' highly private information continuously for over a month. Exhibit 1.

38. In April 2025–approximately one month after Urban One discovered the Data Breach—Defendant finally began notifying some Class Members the Data Breach. *Id.*

39. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

40. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing current and former employees' PII, as evidenced by the Data Breach and its failure to detect the Data Breach for over a month.

41. Urban One's failure to maintain reasonable security safeguards is all the more egregious considering it previously informed California regulators of a data breach in 2019 that involved the theft of more than 1,000 Social Security numbers.[8] In 2019, Urban One promised "it is taking steps, including strengthening its network security posture, to prevent a similar event from occurring in the future" and "Urban One remains dedicated to protecting the sensitive information in its control."[9]

42. Additionally, Defendant did not follow industry standard practices regarding data retention and deletion. Defendant had no business maintaining Plaintiff's PII, considering she is a former employee of Urban One.

---

[8] *Submitted Breach Notification Sample,* ROB BONTA ATTORNEY GENERAL https://oag.ca.gov/ecrime/databreach/reports/sb24-146060 (last visited May 5, 2025)
[9] *Id.*

43. Defendant claims that it has "taken steps to prevent a recurrence," just like it claimed it had done in 2019. However, aside from vaguely claiming it has "increased monitoring, further improved security controls, and reinforced our systems," it has not disclosed what additional controls it has implemented, if any, to improve its security in response to the Data Breach.

44. The risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is substantially high given that the data stolen includes Social Security numbers. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII (although in Plaintiff's case, her Social Security number was compromised). Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff and the Class's financial accounts.

46. On information and belief, Defendant failed to adequately train its IT and data security patients on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII. Defendant's negligence is evidenced by its failure to detect the Data Breach for over a month, failure to prevent the Data Breach (despite promising in 2019 it was taking steps to prevent a reoccurrence), and failure to stop cybercriminals from accessing the PII it stored in its network.

47. Furthermore, Defendant obfuscates the nature of the breach, failing to clearly inform the public the extend of the data that was comprised, whether financial account information was stolen, why it took Defendant over a month to detect the Data Breach in the first place, and

whether Defendant paid a ransom to retrieve the stolen data back, and why Defendant delayed in notifying victims.

Cactus Obtained the PII of Plaintiff and the Class and Posted it for Sale on the Dark Web

48. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class Members' PII for theft and sale on the Dark Web.

49. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII appear to be the notorious cybercriminal group "Cactus."[10]

50. Cactus is a ransomware gang that began claiming responsibility for cyberattacks in April 2023. Its double-extortion scheme involves both stealing data and locking down target systems, then demanding ransom both to unlock systems and to delete stolen data.[11]

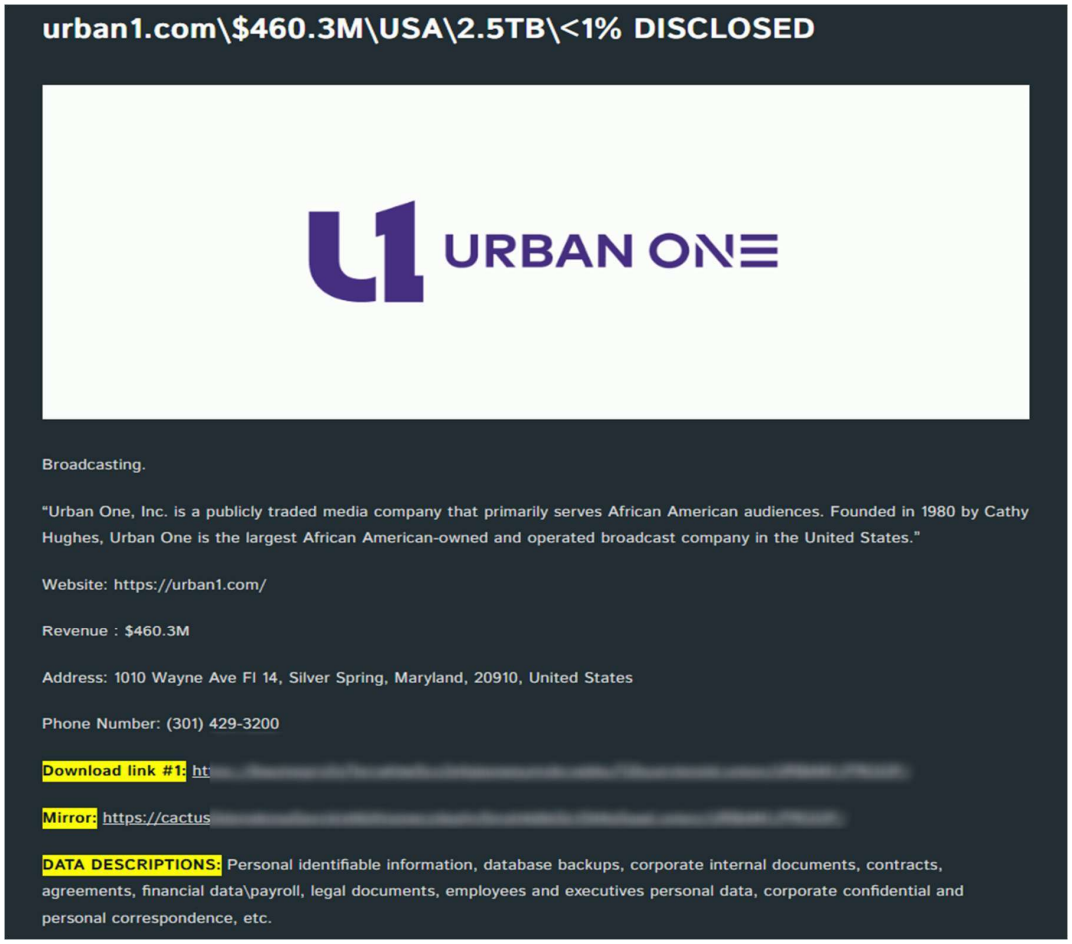
51. Cactus has claimed 46 confirmed ransomware attacks since it started posting targets to its data leak site, plus 191 unconfirmed claims that haven't been acknowledged by the targeted organizations. Other recently confirmed claims made by Cactus include: Kinsey's Archery Products notified 1,330 people of a January 2025 data breach; Athena Cosmetics notified 422 people of a January 2025 data breach; Tempel steel Company was attacked by Cactus in February 2025; and Assa Abloy (Sweden) was hit by Cactus in March 2025.[12]

[10] Paul Bischoff, *Urban One notifies hundres of data breach that comprised SSNs, tax and financial info* (April 23, 2025), COMPARITECH, https://www.comparitech.com/news/urban-one-notifies-hundreds-of-data-breach-that-compromised-ssns-tax-and-financial-info/ (last visited May 5, 2025).
[11] *Id.*
[12] *Id.*

52. On or around March 12, 2025, Cactus claimed credit for the Data Breach in a post on its Dark Web website.[13]

53. Cactus alleges 2.5 TB of data were exfiltrated, including personal identifiable information, database backups, corporate internal documents, contracts, agreements, financial data/payroll, legal documents, employees and executives' personal data, corporate confidential and personal correspondence, etc.

54. A screenshot of some of the data it posted to its Dark Web website is copied below:



[13] *Hack Tuesday*, HACKMANAC, https://hackmanac.com/news/hack-tuesday-week-12-18-march-2025 (last visited May 5, 2025); *Urban One,* BREACHSENSE, https://www.breachsense.com/breaches/urban-one-data-breach/ (last visited May 5, 2025).

55. As seen above, Cactus' post provides a link to download confidential documents from Urban One's network.[14]

56. Thus, on information and belief, INC Ransom has ***already leaked*** the stolen PII of thousands of Defendant's current and former employees.

57. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

58. Therefore, upon information and belief, Urban One intentionally downplays the severity of the Data Breach and the threat it poses to thousands of individuals.

Defendant Knew—or Should Have Known—of the Risk of a Data Breach

59. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

60. Defendant knew, first hand, the severe consequences data breaches can have, considering it was previously subject to a data breach.

61. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

62. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[15]

63. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack. As one report explained, "[e]ntities like smaller

[14] *@H4ckManac Cyberattack Alert* (March 12, 2025), X, https://x.com/H4ckManac/status/1899769568156844467/photo/1 (last visited May 5, 2025).

[15] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited May 5, 2025).

municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

64. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the entertainment industry, including Defendant.

65. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure in its privacy policy, in the instant data breach notice, and in the data breach notice from 2019, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

66. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included extortion and threatening to release stolen data.

67. In light of the information readily available and accessible before the Data Breach, Defendant, knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

Plaintiff's Experience and Injuries

68. Plaintiff is a former employee of Defendant and a Data Breach victim.

[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited May 5, 2025).

69. As a condition of receiving employment, Defendant required Plaintiff to provide her PII, including at least her name, address, Social Security Number, and direct deposit information.

70. Plaintiff provided her PII to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

71. Additionally, Plaintiff reasonably expected that her personal information would be destroyed once her employment with Defendant ended.

72. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

73. Indeed, given Cactus' Dark Web post combined with the Notice Plaintiff has received, Plaintiff's PII has already been published, or will be published imminently by cybercriminals for further theft and sale on the Dark Web.

74. Plaintiff does not recall ever learning that her PII was compromised in former a data breach incident, other than the breach at issue in this case.

75. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Data Breach.

76. Plaintiff suffered actual injury from the exposure of her PII —which violates her rights to privacy.

77. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

78. Additionally, following the Data Brach, Plaintiff experienced a substantial increase in spam phone calls and text messages.

79. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring her credit information.

80. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Plaintiff is experiencing anxiety, distress, and fear regarding how the exposure and loss of her Social Security number will impact him. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

81. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

82. Following the Data Breach, Plaintiff has experienced a substantial increase in scam and spam text messages and emails, some of which address her by name.

83. Once an individual's PII is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[17] On information and belief, Plaintiff's name, Social Security number, and financial information were compromised as a result of the Data Breach.

84. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession despite the fact she is no longer employed by Defendant, is protected and safeguarded from future breaches.

[17] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited May 5, 2025).

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

85. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

86. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

87. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

88. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

89. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

90. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

91. One such example of criminals using PII for profit is the development of "Fullz" packages.

92. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

93. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII

stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

94. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, extortion, and exposure of stolen PII.

95. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest opportunity to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

96. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[18] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer

[18] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

respondents saying they won't purchase from an organization they don't trust with their data."[19]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[20]

c. 89% of consumers stated that "I care about data privacy."[21]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[22]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[23]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[24]

Defendant Failed to Adhere to FTC Guidelines

97. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

98. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

[19] *Id*. at 3.
[20] *Id*.
[21] *Id*. at 9.
[22] *Id*.
[23] *Id*.
[24] *Id*. at 11.

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

99. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

100. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

101. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

102. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

103. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

104. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

105. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

106. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

107. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),

individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach of Urban One, Inc.'s network, including all those individuals who received notice of the breach.

108. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

109. Plaintiff reserves the right to amend the class definition.

110. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

111. This action satisfies the numerosity, commonality, typicality, and adequacy requirements.

112. **Numerosity.** The Class members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 2,157 members.

113. **Commonality and Predominance.** Plaintiff's and the Class Members' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant was negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

114. **Typicality.** Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

115. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's common interests. her interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

116. **Appropriateness.** The likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case.

Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

117. **Ascertainability.** All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some victims and sent them data breach notices.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

118. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

119. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

120. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

121. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

122. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class Members' PII.

123. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

124. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

125. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

126. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

127. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of employment from Defendant.

128. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

129. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and Class Members' and the importance of exercising reasonable care in handling it.

130. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

131. Defendant breached these duties as evidenced by the first and second Data Breach.

132. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff 'and Class Members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

133. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

134. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

135. Defendant has admitted that the PII of Plaintiff and the Class was accessed by an intruder to its systems.

136. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

137. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

139. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

140. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

141. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

142. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

143. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

144. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

145. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

146. Defendant's violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

147. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

149. Defendant offered to provide employment and/or services to Plaintiff and members of the Class if, and in exchange, Plaintiff and members of the Class provided Defendant with their PII.

150. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized persons.

151. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for Defendant's services.

152. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

153. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

154. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusions into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

155. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

156. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

157. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

158. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

159. Defendant failed to advise Plaintiff and members of the Class of that there was not one but two Data Breach, and failed to send Notice to the victims promptly and sufficiently.

160. In these and other ways, Defendant violated its duty of good faith and fair dealing.

161. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

162. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

163. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

164. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

165. Upon information and belief, Defendant funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

166. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

167. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they either provided services, in the form of employment, or purchased services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

168. Defendant knew that Plaintiff and Class Members conferred a benefit which

Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

169. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

170. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiff and the Class by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

171. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

172. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

173. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant either directly or through their own financial institutions.

174. Plaintiff and Class Members have no adequate remedy at law.

175. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

176. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

177. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

178. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

179. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

180. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

181. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person. It constitute an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

182. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

183. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

184. Defendant knowingly did not notify Plaintiff's and Class Members in a timely fashion about the Data Breach.

185. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

186. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

187. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

188. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their PII. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

189. Plaintiff and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

190. Plaintiff and Class Members seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

191. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

192. Given the relationship between Defendant and Plaintiff and the Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff and Class Members of the Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

193. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

194. Because of the highly sensitive nature of the PII, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known

the reality of Defendant's inadequate data security practices.

195. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

196. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach within a reasonable and practicable time period.

197. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

198. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

199. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

200. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

201. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. That to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures;

d. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

e. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

202. The Court should also issue corresponding injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) immediately provide adequate life-time credit monitoring to all Class Members; and (iv) barring Defendant from disclosing the PII/PHI of Plaintiff and the Class without their consent.

203. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

204. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

205. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

206. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class, and naming Plaintiff as representatives of the Class, and Plaintiff's attorneys as Class Counsel;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the putative Class, demands a trial by jury on all claims so triable.

Dated: May 5, 2025

By: */s/ Duane O. King*

Duane O. King Bar No: 19430
THE LAW OFFICES OF DUANE O. KING, PC
803 W. Broad St., Suite 210
Falls Church, VA 22046
Telephone: (202) 331-1963

dking@dkinglaw.com

Raina C. Borrelli (*pro hac vice* anticipated)
STRAUSS BORRELLI, PLLC
980 N. Michigan Ave., Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class